

## 明細書

### 発明の名称

### 暗号強度評価装置

### 技術分野

本発明は、暗号強度評価装置に関する。

### 背景技術

暗号化と復号化に同一の共通鍵を用いる共通鍵方式には、例えばデータをブロックに区切り、ブロック毎に暗号化する方式のブロック暗号があり、このブロック暗号の中には、DES や MISTY 等の共通鍵から算出される拡大鍵をパラメタに用いた攪拌を繰り返し行うことで平文を段階的に暗号化するものがある。

暗号が社会で安全に利用できることを示すために、実際に暗号の解読を試みるにより評価が行われる。この暗号の解読法としては、例えば、推定される全ての鍵について暗号化または復号化を行い、一対の平文と暗号文があれば鍵を求めることができる全探索法や、2 対の平文と暗号文の、平文間の排他的論理和と、暗号文間の排他的論理和との間に高い確率で関係が成り立つ場合に、攪拌の最終段階で用いられる拡大鍵を求めようとする差分解読法、又、攪拌の最終段階で出力される暗号文を平文のブール多項式を用いて表し、このブール多項式の高階差分を定数にすることで拡大鍵を推定する条件とし、代数的手法等で拡大鍵を求める高階差分解読法等が知られている。

しかし、現在これらはいずれも一つの鍵を求めることを目的として適用されており、より厳密な暗号に関する評価を行うために複数の段階の拡大鍵を求めようとしたとき、各段階に単にこれらを適用するのであれば、計算量の削減を行うことにはならない。

### 非特許文献

文献 1 : Babbage, Frisch, "On MISTY1 Higher Order Differential Cryptanalysis", 3<sup>rd</sup> International Conference on Information Security and Cryptology 2000

- 文献 2 : Daemon,Knudsen,Rijmen,"The BlockCipher SQUARE",FSE-6<sup>th</sup> ]①  
International Workshop LNCS.1636
- 文献 3 : Jakobsen,Knudsen,"The Interpolation Attack on Block Cipher",FSE-4<sup>th</sup> International Workshop,LNCS.1372
- 文献 4 : Knudsen,"Truncated and Higher Order Differentials",FSE-2<sup>nd</sup> International Workshop,LNCS.1008
- 文献 5 : Lai,"Higher Order Derivatives and Differential Cryptanalysis",Communications and Cryptography
- 文献 6 : Matsui,"New Structure of Block Ciphers with Provable Security against Differential and Linear cryptanalysis",FSE-3<sup>rd</sup> International Workshop,LNCS.1039
- 文献 7 : Moritai,Shimoyama,Kaneko,"Higher Order Attack of a CAST Cipher", FSE-4<sup>th</sup> International Workshop,LNCS.1372
- 文献 8 : Nyberg,Knudsen,"Provable Security against Differential Cryptanalysis",Journal of Cryptology,Vol.8-no.1
- 文献 9 : Shimoyama,Moriai,Kaneko,"Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher", 1997 Information Security Workshop,LNCS.1396
- 文献 10 : Tanaka,Hisamatsu,Kaneko,"Strength of MISTY1 without FL function for Higher Order Differential Attack",13<sup>th</sup> International Symposium,Applied Algebra-Algebraic Algorithms and Error-Correcting Codes 1999,LNCS.1719

#### 発明の開示

そこで本発明は、複数段階の拡大鍵をまとめて求めるに関して計算量等の削減を行うことを目的としたものである。

すなわち本発明にかかる暗号強度評価装置は、平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪

拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文についての強度の評価を行う暗号強度評価装置であって、

②  
M4

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられる前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文を出力させるものであることを特徴とする。

このようなものであれば、個別に各段階の鍵を求めていくよりも、複数の候補を算出しておき、前の段階の鍵の算出過程で絞り込む方が計算量などを削減

。することができる場合に効果がある。また、各段階の拡大鍵候補を全て算出し終えてから前の段階の拡大鍵候補を算出するよりも、ある一つの拡大鍵候補を拡大鍵であると仮定して前の段階の拡大鍵を求める方が、早い段階で複数の拡大鍵を発見することができる。

③  
M

同様の効果を奏するものとしては、平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文についての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文

と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より  
出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文を出力させるものを挙げることができる。

④  
148

このようなものであれば、ある段階の拡大鍵と等しいと推定される一つの拡大鍵候補について、前の段階の拡大鍵候補を求めるのに、当該段階の拡大鍵候補などに基づいて最適な前の段階の拡大鍵候補を算出する条件を構成することができ、計算量等を削減することができる。

また、平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある2つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不能を識別し、算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推

定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

⑤

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文を出力させるものでもかまわない。

このようなものであれば、例えばある段階の拡大鍵候補の算出に用いる条件に、冗長な条件等を追加することで複数の条件として構成しておき、その条件から、例えばこれらの条件を満たす拡大鍵は一つも存在しない等の矛盾を判断することで、実際に前の段階の拡大鍵を算出してみることなく当該拡大鍵候補が偽であることを識別することができる。

更に、平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

第1未攪拌文算出部と、第2未攪拌文算出部と、制御部とを備えており、更に第1未攪拌文算出部は未攪拌文算出部本体と、第1拡大鍵候補算出部とを備えたものであり、第2未攪拌文算出部は第2拡大鍵候補算出部を備えたものであり、

前記第1未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記第2未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される

推定撹拌文とを受け付けるものであり、]⑥ ㍉

前記第1拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定撹拌文とを用いて、ある撹拌段階で用いられる前記拡大鍵の全探索を行い、当該段階での撹拌に用いられるの前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記第2拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定撹拌文とを用いて、高階差分解読法を適用することで当該段階での撹拌に用いられるの前記拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる複数の条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある2つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不能を識別し、算出不能を示す算出不能識別データを出力するものであり、

未撹拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定撹拌文に基づいて当該段階で未だ撹拌されていない未撹拌文と等しいと推定される推定未撹拌文を算出し、未撹拌文算出部の出力として出力するものであり、

制御部が、対を成す前記平文と、撹拌の最終段階の前記暗号文又はある中間段階の前記推定撹拌文とを前記第1未撹拌文算出部へ入力し、出力される前記推定未撹拌文を受け付け当該段階の前段階の前記推定撹拌文として、前記平文と共に更に前記第2未撹拌文算出部へ入力し、又、前記第2拡大鍵算出部より出力される前記算出不能識別データを受け付けることで、前記再算出要求データを前記第1拡大鍵算出部へ出力し、前記第1拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未撹拌文を出力させるものであれば、

2種類の拡大鍵算出部を用い、ある段階で高階差分解読法を用いた代数的な手法の条件を動的に構成することで、条件に基づいて実際に拡大鍵の算出を行うことなく当次の段階の拡大鍵候補が偽であること識別し、例えば MISTY1

と同様の攪拌部を持つ暗号であれば、次の段階では負荷の高い全探索を利用しているにも関わらず2段以上の拡大鍵を求める場合にも総合的には計算量を削減できる。

#### 図面の簡単な説明

##### 図 1

本願発明の請求項 1、請求項 2、請求項 3 に関する機能を示す機能構成図

##### 図 2

本願発明の請求項 4 に関する機能を示す機能構成図

##### 図 3

本発明の実施形態におけるハードウェア構成図

##### 図 4

同実施形態における暗号強度評価装置の機能構成図

##### 図 5

M I S T Y 1 における機能構成図

##### 図 6

変形 M I S T Y 1 における機能構成図

##### 図 7

変形 M I S T Y 1 における次数の増加に関する形式的な分析結果を含むの攪拌部（F O 関数）の機能構成図

##### 図 8

変形 M I S T Y 1 における鍵  $\kappa$  の変形過程

発明を実施するための最良の形態

以下、本発明の実施の形態について説明する。

図 2 は、この実施の形態における暗号強度評価装置を示した機器構成図である。この暗号強度評価装置は、同図が示すように、例えば汎用コンピュータであり、図 3 に示すように、C P U 1 0 1、内部メモリ 1 0 2、H D D 等の外部記憶装置 1 0 3、通信ネットワークに接続するためのモデム等の通信インタフェース 1 0 4、ディスプレイ 1 0 5、マウスやキーボードといった入力手段 1 0 6 等



を具備する。] ⑧ 18x

しかして本実施形態では、図4に示すように、前記暗号強度評価装置に所定のプログラムをインストールし、そのプログラムに基づいてCPU101や周辺機器を共働させることにより、この暗号強度評価装置が、平文暗号文算出部3及び制御部1、第1推定未攪拌文算出部21、第2推定未攪拌文算出部22、未攪拌文算出部本体20A、第1拡大鍵候補算出部21K、第2拡大鍵候補算出部22K、として機能するようにしている。

図5に示すようにMISTY1は128ビットのユーザ鍵を用いて、64ビットの平文から64ビットの暗号文を生成するブロック暗号であり、8段階を成すFO関数と呼ばれる攪拌部と、線形なFL関数から構成されている。攪拌部は、3つの攪拌中間要素であるFI関数を備えており、攪拌中間要素は、更に3つの攪拌要素であるSボックスを備えている。本実施形態は図5に示すFL関数の無い図6に示す6段のMISTY1（以下では変形MISTY1と呼ぶ）について暗号強度の評価をおこなう目的で構成している。

各部を詳述する。

高階差分解読法により得られるブール多項式の次数は選択する平文に依存している。次数は必要な選択平文の数や計算量に影響を与えるため、効果的な平文を選択することは重要である。

平文は、変形MISTY1に設けられた攪拌部の要素であるSボックスS7、S9により8つの部分ブロックに分割される。

$$P = (X_7, X_6, \dots, X_1, X_0), \quad X_i \in \begin{cases} \text{GF}(2)^7, & i = \text{even} \\ \text{GF}(2)^9, & i = \text{odd}. \end{cases}$$

出力の次数は、どのような部分ブロックを入力として選択したかに依存する。

変形MISTY1に関して効果的な平文を調べた結果、次数の増加がゆるやかな、効果的な平文を探した結果、右端の部分ブロックだけを変化させ、残りを固定することで得られる平文が効果的であることが解ったので、平文暗号文算出部3はこのような条件を満たす平文と暗号文の対を算出するように構成

した。]⑨ *W*

図7は形式的な分析により、この平文に関する次数の増加を表したものである。< i / j >という表現は、左側のブロックが i であり、右側のブロックが j であることを示している。

第1推定未攪拌文算出部21は前記平文暗号文算出部より出力される平文と、暗号文とを受け付け、第5段の推定未攪拌文を出力するものであり、その内部には第1拡大鍵候補算出部と、推定未攪拌文算出部本体とを設けている。

第1拡大鍵候補算出部は全探索を用い、第6段の1つの拡大鍵候補を求め算出する。

また、再算出を要求する再算出要求データを受け付けることで出力済の拡大鍵候補とは異なる新たな当該段階の拡大鍵候補を算出を試み、算出できた場合には新たな拡大鍵候補を出力するが、拡大鍵候補を全て算出し終え、新たな拡大鍵候補を算出できなくなった場合には、算出不能を示す算出不能識別データを出力する。

未攪拌部算出部本体は、前記の一つの拡大鍵候補を用いて MISTY1 の第6段の未攪拌文を出力する。これは復号化で用いられるのと同じ手順で行う。

第2推定未攪拌文算出部22は前記平文暗号文算出部3より出力される平文と、暗号文とを受け付け、第5段の拡大鍵候補の出力を確認するものであり、その内部には第2拡大鍵候補算出部を設けている。

第2拡大鍵候補算出部では、まず入力された推定攪拌鍵に基づいて動的に拡大鍵候補を算出するための複数のブール多項式を構成する。

ここで、高階差分解読法より成り立つ、次の2つの性質を用いる。

特性1:

$$\deg_X \{F(X; K)\} = d \Rightarrow \begin{cases} \Delta^{(d+1)} F(X; K) = 0 \\ \Delta^{(d)} F(X; K) = \text{const} \end{cases} \quad (1)$$

特性2:      Let  $F(X) : \text{GF}(2)^n \mapsto \text{GF}(2)^n$ . If  $V_{\{a_0, a_1, \dots, a_{n-1}\}} = \text{GF}(2)^n$ , then for any fixed value  $f \in \text{GF}(2)^n$ ,  $\Delta^{(n)} F(X + f; K) = \Delta^{(n)} F(X; K)$ .

平文暗号文算出部より出力される平文には7ビットの変数が含まれる。7階

差分を用いた解読法を用いるのに、まず部分空間  $V^{(7)}$  を次のように定める。] ⑩  $\mu$

$$V^{(7)} = V_{\{a_0, a_1, \dots, a_6\}}, \quad a_i = (0, 0, \dots, 1, \dots, 0) \in \text{GF}(2)^{64}$$

↑  $i$ -th bit (2)

以下では、 $V^{(7)}$  がわかっているときには  $\Delta^{(7)}_{[a_0, a_1, \dots, a_6]}$  を  $\Delta^{(7)}$  と表すことにする。

$H^{L7}_{32}$  を  $\text{FO}_3$  の出力の左の 7 ビットとすると

$$H^{L7}_{32} = H_{312} + H_{322} + Z_{322}. \quad (3)$$

特性 1 より次の条件が成り立つ。

$$\begin{aligned} \Delta^{(7)} H^{L7}_{32} &= \Delta^{(7)} (H_{312} + H_{322} + Z_{322})]_7 \\ &= \Delta^{(7)} H_{312}]_7, \end{aligned} \quad (4)$$

“]d” は  $d$  次未満の項を省く操作を示している。

$F(\cdot)$  は図 7 に示される  $\text{GF}(2)^7 \times \text{GF}(2)^9 \mapsto \text{GF}(2)^7$  とする関数であり

$$H_{312} = \mathcal{F}(X_0 + H_{133} + K_{222}, Y_{221}). \quad (5)$$

となる。

$Y_{221}$  は選択した平文に関して一定である。 $X_0$  は  $\text{GF}(2)^7$  を張るので、特性 2 より次の条件が成り立つ。

$$\begin{aligned} \Delta^{(7)} H_{312} &= \Delta^{(7)} \mathcal{F}(X_0 + H_{133} + K_{222}, Y_{221}) \\ &= \Delta^{(7)} \mathcal{F}(X_0, Y_{221}) \end{aligned} \quad (6)$$

そして式(22)と式(24)より  $H^{L7}_{32}$  の 7 階差分が次のように求まる。

$$\Delta^{(7)} H^{L7}_{32} = \Delta^{(7)} \mathcal{F}(X_0, Y_{221})]_7. \quad (7)$$

$H_{312}$  のブール多項式を調べることで、 $H_{312}$  は次数が 7 であり、 $H^{L7}_{32}$  の 7 階差分は 0x6D となり、6 次の項の係数は  $Y_{221}$  の要素の関数であることがわかった。

$$X_{222} = (x_6, \dots, x_0), \quad (X_{222} = X_0 + H_{133} + K_{222})$$

$$Y_{221} = (y_8, \dots, y_0), \quad H_{312} = (\hat{h}_6, \dots, \hat{h}_0)$$

$\Delta^{(7)} H^{L7}_{32} = 0x6D$  より、次の条件が生成される。

$$\sum_{A \in V^{(7)}} \{FO(C_L(P+A) + \kappa_L; K_{522}, K_{521}, K_{512}, K_{511}) \\ + C_R(P+A) + \kappa_R\}$$

$$= 0x6D$$

$$\kappa = (\kappa_L, \kappa_R), \quad \kappa_L, \kappa_R \in GF(2)^{32} \quad (8)$$

鍵  $\kappa$  は図 8 のようにして変形される。 $\kappa_L$  は FO5 関数で  $\kappa_{Ll}$  と  $\kappa_{Lr} (\in GF(2)^{16})$  に分割されるので、FI<sub>51</sub> で以下の条件が成り立つ。

$$\begin{aligned} \kappa_{511} &= K_{511} + \kappa_{Li}^{L9} \\ \kappa_{512} &= K_{512} + \kappa_{Li}^{R7} \end{aligned} \quad (9)$$

また FI<sub>52</sub> で以下の条件が成り立つ

$$\begin{aligned} \kappa_{521} &= K_{521} + \kappa_{Lr}^{L9} \\ \kappa_{522} &= K_{522} + \kappa_{Lr}^{R7} \end{aligned} \quad (10)$$

ゆえに、条件(8)は次のように変形できる。

$$\begin{aligned} &\sum_{A \in V^{(7)}} \{FO(C_L(P+A); \kappa_{522}, \kappa_{521}, \kappa_{512}, \kappa_{511}) \\ &\quad + C_R(P+A)\} \\ &= 0x6D \end{aligned} \quad (11)$$

このようにして得られた条件(11)を代数的な方法（文献 7,9 参照）で線形な複数の条件に構成し、第 2 拡大鍵候補算出部 2 2 K での拡大鍵候補の算出に用いる条件とする。

もし、複数の拡大鍵候補の算出の条件に、互いに矛盾する条件がこの複数の条件に含まれるのであれば第 2 拡大鍵候補算出部 2 2 K は拡大鍵候補の算出不能を示す算出不能識別データを出力する。

また、本実施例では第 6 段階及び第 5 段階の拡大鍵を求めることで評価することを目的とするため、第 2 拡大鍵候補算出部 2 2 K で構成する、拡大鍵候補の算出に用いる条件に十分な冗長性を持たせ、拡大鍵候補が真となるように構成してある。

制御部は平文暗号文算出部の出力する、対を成す平文と、攪拌の最終段階の暗号文とを第 1 未攪拌文算出部へ入力し、出力される第 6 段階の推定未攪拌文

を受付け第5段階の推定撹拌文として、平文と共に更に第2未撹拌文算出部へ  
入力する。又、第2拡大鍵算出部より出力される算出不能識別データを受け付  
けることで、再算出要求データを第1拡大鍵算出部へ出力し、第1拡大鍵算出  
部に再び第6段階の新たな拡大鍵候補を算出させ、この新たな拡大鍵候補に基  
づいて第5段階の推定未撹拌文を出力させるように構成されている。

このように構成された暗号評価装置を用いて、変形MISTY1の出力する  
暗号に関わる評価を行う手順を以下に示す。

あらかじめ平文暗号文算出部3に、評価の対象である変形MISTY1に高  
階差分解読法を適用するために都合の良い平文と暗号文の対を定める条件を  
設定しておく。

平文暗号文算出部3は設定した条件を満たす平文と暗号文の対を生成し出  
力する。

制御部1は平文暗号文算出部3の出力する平文と暗号文をと前記第1未撹  
拌文算出部21へ入力する。

第1未撹拌文算出部21は入力された平文と暗号文とを受け付け、第1未撹  
拌文算出部21に設けた第1拡大鍵候補算出部21Kが、暗号化のパラメタで  
ある第6段階の拡大鍵の候補である拡大鍵候補の一つを全探索の手法を用い  
て算出する。

第1未撹拌文算出部21Kに設けられた未撹拌文算出部本体20Aは、この  
算出された拡大鍵候補を用いて前記暗号文を復号化することで、変形MIST  
Y1の撹拌の最終段階である第6段階での撹拌を、未だ施していない状態であ  
る第6段階の出力と等しい推定される推定未撹拌を算出し、第1未撹拌文算出  
部21の出力として出力する。

そして制御部1は、出力される第6段階の推定未撹拌文を受け付け第5段階  
の推定撹拌文として、平文と共に更に第2未撹拌文算出部22へ入力する

第2未撹拌文算出部22は入力された平文と第5段階の推定撹拌文とを受  
け付け、第2未撹拌文算出部22に設けた第2拡大鍵候補算出部22Kが、第  
5段階の推定撹拌文を用いて動的に第5段階の拡大鍵候補を算出するための

条件を構成し、代数的手法で算出を行うか、又は、互いに矛盾する条件が存在すれば算出不能識別データを出力する。

⑫  
As

制御部 3 は出力される算出不能識別データを受付けることで、再算出要求データを第 1 拡大鍵算出部 2 1 K へ出力する。

第 1 拡大鍵算出部 2 1 K は出力された再算出要求データを受け付け再び新たな第 6 段階の拡大鍵候補を算出し、新たに算出された第 6 段階の拡大鍵候補に基づいて第 6 段階の推定未攪拌文を出力させる。

このようにして、第 5 段階の拡大鍵候補が算出されるまで第 6 段階の拡大鍵候補の算出を繰り返す。最終的に得られる第 5 段階の拡大鍵候補は確率的に拡大鍵と等しいとみなせるため、算出までにかかった計算量や用いた対の平文と暗号文の数は暗号の強度を評価する指標としてディスプレイに表示する。

なお、本発明は、前記実施形態に限られるものではない。

まず、評価を行う対象は、変形 M I S T Y 1 や、M I S T Y 1 の攪拌部を用いたものに限らない。

更に多くの段階の拡大鍵を求めるために、更に新しい攪拌文算出部を設けても良いし、既存の攪拌文算出部を繰り返して用いても構わない。

また、拡大鍵候補の算出に全探索や高階差分解読法を適用する代わりに、差分解読法、線形解読法等の解読法を適用してももちろん構わない。

また、平文と暗号文の算出するために、例えば平文又は暗号文を、評価者がキーボード等の入力手段を用いて平文暗号文算出部に設定する構成とすれば、例えば評価を行うのに都合の良い平文と暗号文の組が満たす条件を、試行錯誤して見つけるのに便利であるし、平文または暗号文をネットワークや他のプログラムからの入力として受け付けるように構成すれば、例えば新たに評価に用いる平文及び暗号文を個々の暗号強度評価装置に振り分け入力する分散処理管理プログラムと共に用いることで、並列的に暗号を評価することができる。

また、ある推定未攪拌文算出部より出力される推定未攪拌文を異なる暗号強度評価装置の入力として用いるか、又は異なる暗号強度評価装置の出力する推定未攪拌文を本暗号評価装置のある推定未攪拌文算出部の入力とすることで、

例えば異なる攪拌段階を複合的に用いた暗号にも適用することが可能となる。]

(13)  
24

以上のように上述した暗号強度評価装置を用いることで変形MISTY1は7階差分を用いることで解説可能となることを示すことができた。

この暗号強度評価装置により、第6段階のサブキーに全探索を適用し、第5段階のサブキーの一部に代数的解説法を適用することで、 $2^{12}$ の選択した平文と $2^{93}$ 回のF関数の演算が必要となったが、計算量の削減の効果により、128ビットのユーザ鍵に対して全探索を適応するよりも、推定でおよそ $2^{30}$ 倍早く評価を終えることができ、暗号方式としてMISTY1を用いるには少なくとも7段階でなければ高階差分解読法により解説される可能性があることを示すことができた。

## 特許請求の範囲

1. 平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられる前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文



を出力させるものである暗号強度評価装置。]

(14) 18

2. 平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文についての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文

を出力させるものである暗号強度評価装置。

⑮

3. 平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文についての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある2つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不能を識別し、算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡

大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文] (16)  
を出力させるものである暗号強度評価装置。 147

4. 平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文についての強度の評価を行う暗号強度評価装置であって、

第1未攪拌文算出部と、第2未攪拌文算出部と、制御部とを備えており、更に第1未攪拌文算出部は未攪拌文算出部本体と、第1拡大鍵候補算出部とを備えたものであり、第2未攪拌文算出部は第2拡大鍵候補算出部を備えたものであり、

前記第1未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記第2未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記第1拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、ある攪拌段階で用いられる前記拡大鍵の全探索を行い、当該段階での攪拌に用いられるの前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記第2拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、高階差分解読法を適用することで当該段階での攪拌に用いられるの前記拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる複数の条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある2つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不

能を識別し、算出不能を示す算出不能識別データを出力するものであり、

①⑦

未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される推定未攪拌文を算出し、未攪拌文算出部の出力として出力するものであり、

制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記第1未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に前記第2未攪拌文算出部へ入力し、又、前記第2拡大鍵算出部より出力される前記算出不能識別データを受け付けることで、前記再算出要求データを前記第1拡大鍵算出部へ出力し、前記第1拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文を出力させるものである暗号強度評価装置。